the HSAR. Component desiring to use a provision or a clause on a standard basis shall submit a request containing a copy of the clause(s), justification for its use, and evidence of legal counsel review to the CPO in accordance with (HSAR) 48 CFR 3001.304 for possible inclusion in the HSAR.

(B) Provisions and clauses used on a one-time basis (i.e., non-standard provisions and clauses) may be approved by the contracting officer, unless a higher level is designated by the Component. This authority is subject to:

(*1*) Evidence of legal counsel review in the contract file;

(*2*) Inserting these clauses in the appropriate sections of the uniform contract format; and

(*3*) Ensuring the provisions and clauses do not deviate from the requirements of the FAR and HSAR.

NOTE TO 3052.101: The solicitation provisions and contract clauses matrix referencing all HSAR provisions and clauses is available at *http://www.dhs.gov/xopnbiz/* under Policy and Regulations, Homeland Security Acquisition Regulation (HSAR).

[68 FR 67871, Dec. 4, 2003, as amended at 71 FR 48802, Aug. 22, 2006; 77 FR 50636, Aug. 22, 2012]

Subpart 3052.2—Text of Provisions and Clauses

3052.203–70 Instructions for Contractor Disclosure of Violations.

As prescribed in (HSAR) 48 CFR 3003.1004(a), insert the following clause:

INSTRUCTIONS FOR CONTRACTOR DISCLOSURE OF VIOLATIONS (SEP 2012)

When making a written disclosure under the clause at FAR 52.203–13, paragraph (b)(3), the Contractor shall use the Contractor Disclosure Form at *http://www.oig.dhs.gov* and submit the disclosure electronically to the Department of Homeland Security Office of Inspector General. The Contractor shall provide a copy of the disclosure to the Contracting Officer by email or facsimile on the same business day as the submission to the Office of Inspector General. The Contractor shall provide the Contracting Officer a concurrent copy of any supporting materials submitted to the Office of Inspector General.

[77 FR 54836, Sept. 6, 2012]

3052.204–70 Security requirements for unclassified information technology resources.

As prescribed in (HSAR) 48 CFR 3004.470–3, insert a clause substantially the same as follows:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within ____ [''insert number of days''] days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 *et seq.*); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A–130.

(3) The securitplan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include—

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

[71 FR 25772, May 2, 2006]

3052.204–71 Contractor employee access.

As prescribed in (HSAR) 48 CFR 3004.470–3(b), insert a clause substantially the same as follows with appropriate alternates:

CONTRACTOR EMPLOYEE ACCESS (SEP 2012)

(a) *Sensitive Information*, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107–296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, ''Policies and Procedures of Safeguarding and Control of SSI,'' as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as ''For Official Use Only,'' which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated ''sensitive'' or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) ''Information Technology Resources'' include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that